IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): James Kleinsteiber, Richard L. Hammons, Dilip Gunawardena, Hung Nguyen, Shankar Balasubramanian, and Vidya Renganararayanan	§	Confirmation No.: 2526
Serial No.: 10/062,125	§	Art Unit: 2131
Filed: January 21, 2002	§	Examiner: Matthew T. Henning
For: Network Security and Applications to the Fabric Environment	§	Attorney Docket No.: 112-0039US
	§	Customer No.: 29855

Box Appeal Brief
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Mail Stop: Appeal Briefs – Patents

APPEAL BRIEF

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Brocade Communications Systems, Inc.

II. RELATED APPEALS AND INTERFERENCES

None

III. STATUS OF CLAIMS

Claims 1–61 and 27–87 are rejected. The appealed claims are 1–61 and 72–87.

IV. STATUS OF AMENDMENTS

None filed

V. SUMMARY OF CLAIMED SUBJECT MATTER

This section provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by paragraph and line number and to the drawings by reference characters as required by 37 CFR § 41.37(c)(l)(v). Where applicable, each element of the claims is identified with a corresponding reference to the specification and drawings. Line numbers refer to the published application. Citation to the specification and/or drawings does not imply that limitations from the specification and drawings should be read into the corresponding claim element. Additionally, references are not necessarily exhaustive, and various claim elements may also be described at other locations.

One aspect claimed is a method of operating a secure network. The method includes:

- Locating one or more nodes in a secure location (¶ 77, ll. 3–11; ¶ 80, ll. 20–27; Fig. 10, element 1027).
- Locating one or more nodes in a less secure location (¶ 63, ll. 1–12; ¶ 77, ll. 1–11).
- Communicating selected management information from a primary configuration node to all other nodes in the secure network, (¶ 80, ll. 27–30) said communicating having the substeps of:
    - A first port on a first node sending said management information to a second port on a second node via a communication media exclusively shared by said first port and said second port (¶ 80, ll. 1–27; Fig. 10, element 1022);
    - Allowing no management access to said secure network from nodes located in said less secure locations (¶ 63, ll. 7–12; ¶ 77, ll. 6–9);
    - Determining a first list of nodes that may send or receive substantive communication in the secure network (¶ 126–30); and
    - Prior to substantive communication between any two directly-connected ports, authenticating a link between said directly connected ports (¶ 169, ll. 3–7).

A second aspect claimed is a networking node in a secured network. The networking node includes:

- A first port on said specific networking node (*e.g.*, Fig. 10, switch 1001) for receiving selected management information from a primary configuration node (*e.g.*, Fig. 10, element 1022), said first port directly communicating with a second port on a second node via a communication media exclusively shared by said first port and said second port (*e.g.*, link 1017) (*see also*, ¶ 80, ll. 1–27);
- A memory for storing (i) management access information, and (ii) device connection information specifying nodes or ports that may send or receive substantive communication in the secure network (Fig. 2, elements 208, 210; ¶ 126–30); and
- A processor for causing the authentication of the link between said first port and said second port prior to substantive communication between said first and second ports (Fig. 2, element 202);
- Wherein said primary configuration ode is configured or adapted to exclusively control a defined set of management functions throughout said secure network (¶ 80, ll. 1–20).

A third aspect claimed is a method of securing a fabric having a plurality of switches. The method includes:

- Only allowing communication between pre-defined pairs of said switches as specified by a network operator (¶ 66, ll. 1–5; Fig. 1, elements 110, 112, 114, 116); and
- Only allowing substantive communication between devices that are on a pre-defined list of allowed devices, said pre-defined list stored on a memory in each of said plurality of switches (¶ 126–29); and
- Only allowing substantive communication between directly connected ports that have been mutually authenticated (¶ 169, ll. 3–7).

A fourth aspect claimed is a network. The network includes:

- A plurality of devices including one or more switching and routing devices, any two of said devices able to inter-communicate only by direct links between each other, all devices able to inter-communicate by forwarding communications through each other (*e.g.*, Fig. 1);
- All of said devices capable of mutually authenticating directly connected links (¶ 149);
- One or more pre-designated devices for facilitating management-level control of the network (¶ 80–81); and
- All of said devices carrying a list of all devices allowed on the network (¶ 126–30).

A fifth aspect claimed is routing device for receiving and directing information. The network includes:

- A public and private key pair (¶ 154);
- One or more ports for coupling to other routing devices and for authenticating said other routing devices and for communicating using said public and private key pair (Fig. 2, element 220);
- A memory for storing a list of all said other routing devices that are allowed to substantively communicate on the network (Fig. 2, elements 208, 210); and
- At least one logical management access channel that may be disabled through network management control (¶ 115–23).

A sixth aspect claimed is a network configuration entity configured or adapted to exlusively control a defined set of management functions throughout a secure network. The network includes:

- A memory for storing (Fig. 2, elements 208, 210):
    - An NCE list, said NCE list comprising an indication of each device in the network that may operate as said network configuration entity (¶ 82);

  - An SCC list, said SCC list comprising an indication of each device allowed to participate in said secure network (¶ 130);
  - A first secret fact (¶ 161);
- A first port for sending said secret fact to a second switch (Fig. 2, element 220);
- A second port for receiving (Fig. 2, element 220),
  - A second-type derivative of said first secret fact from said second switch,
  - Pre-defined information about said second switch, and
  - A third-type derivative of said pre-defined information about said second switch (¶ 162–63); and
- A processor for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said second switch and said third-type derivative of said pre-defined information about said second switch (Fig. 2, element 202).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1–61 stand rejected under 35 U.S.C. § 112, ¶ 2 for failing to point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1–13, 17–19, 35–47, 51–53, and 73 stand rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent 5,619,657 to Sudama et al. ("Sudama"). Claims 14–16, 20–21, 48–50, and 54–55 stand rejected under 35 U.S.C. § 103(a) as obvious over Sudama. Claims 22–31, 33–34, 56–61, and 76–87 stand rejected under 35 U.S.C. § 103(a) as obvious over Sudama in view of FIPS PUB 196 "Entity Authentication Using Public Key Cryptography" ("FIPS"). Claim 32 stands rejected under 35 U.S.C. § 103(a) as obvious over Sudama and FIPS in view of U.S. Patent 5,422,953 to Fischer ("Fischer"). Claims 72 and 74 stand rejected under 35 U.S.C. § 103(a) as obvious over Sudama in view of U.S. Patent 5,694,615 to Thapar et al. ("Thapar"). Claim 75 stand rejected under 35 U.S.C. § 103(a) as obvious over Sudama in view of applicant admitted prior art.

VII. ARGUMENT

The claims do not stand or fall together. Instead, Appellants present separate arguments for various independent and dependent claims. After a concise discussion of cited art, each of these arguments is separately argued below and presented with separate headings and sub-heading as required by 37 CFR § 41.37(c)(l)(vii). To aid in review of this long and complicated Office Action various rejections have been copied into this brief. Arguments as to the rejection then follow.

A. Section 112, ¶ 2 Indefiniteness Rejections

The Office Action rejected the claims under various § 112, ¶ 1 Indefiniteness grounds. Applicants respectfully traverse all of them.

For example, claims 1 and 13 were rejected for use of the terms "secure location" and "less secure location." The text of the exact rejection is:

> The term "secure location" in claims 1, 13, is a relative term which renders the claim indefinite. The term "secure location" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. In this particular instance, one of ordinary skill in the art would be unable to determine what constitutes "a secure location". For example, would a fireproof room be considered a secure location. Would a room anchored to the earth be considered a secure location. Would a plaza with armed guards be considered a secure location. As such, one of ordinary skill in the art would not be able to determine the scope of the claim. Therefore, claim 1 is rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

> The term "less secure location" in claims 1, 13 is a relative term which renders the claim indefinite. The term " less secure location" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. In this particular instance, one of ordinary skill in the art would be unable to determine what constitutes "a less secure location". For example, would a non-fireproof room be considered a less secure location. Would a room not anchored to the earth be considered a less secure location. Would a plaza with no armed guards be considered a less secure location. Furthermore, the claim gives no basis as to what the location is less secure than. As such, one of ordinary skill in the art would not be able to determine the scope of the claim. Therefore, claim 1 is rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

As noted in a prior response, the specification does provide sufficient guidance for one skilled in the art to determine the meaning of "secure location" and "less secure location." For example, ¶ 16 teaches that:

> [T]he logical security of the entire network may be enhanced by providing greater physical security…. [N]etwork operators … may maintain logical network security while deploying devices in both secure and non-secure physical locations. That is the ability to ***locate network equipment in buildings, rooms or cabinets with varying degrees of physical security as long as the network configuration entity is located in an area of sufficient physical security***.

Similarly, ¶ 63 teaches that "equipment residing in less secure physical environment[s] should present security barriers for effecting the network." Additionally, ¶ 80 teaches that:

> In some implementations, the NCE [Network Configuration Entity] may be reached through any of its normal communications mechanisms, although, higher security may be achieved if the NCE must be directly accessed by an operator. ***The latter case provides enhanced security because physical access to the NCE may be controlled, such as by use of a secure locked room or enclosure***….

Based on the foregoing, as well as other teachings of the specification, Applicants respectfully submit that one skilled in the art would be able to ascertain the meaning of "secure location" as used in claims 1 and 13. MPEP 2173.02 provides that:

> The essential inquiry pertaining to this requirement is whether the claims set out and circumscribe a particular subject matter with a reasonable degree of clarity

> and particularity. Definiteness of claim language must be analyzed, not in a vacuum, but in light of: (A) The content of the particular application disclosure; (B) The teachings of the prior art; and (C) The claim interpretation that would be given by one possessing the ordinary level of skill in the pertinent art at the time the invention was made.

Considering factor "A," the specification gives examples of secure locations (*e.g.*, secure locked rooms or enclosures). By clear implication, less secure locations would include unlocked rooms or enclosures. The specification also gives a standard for determining the level of security required (*e.g.*, that the network configuration entity should be "located in an area of sufficient physical security").

Considering factor "B," examiner points to specific passages of the Sudama reference as purportedly teaching locating one or more nodes in a secure location and locating one or more nodes in a less-secure location. While Applicants' do not concede that Sudama so teaches, the fact that Examiner can ascertain the meaning of the terms sufficiently to identify them in prior art seems to suggest that the claim terms are not indefinite.

Considering factor "C," one skilled in the art would understand that the absolute level of security provided by the secure location is not as important that the level of security at the secure location be sufficient to address some threat to network security that was not addressed by the less-secure location (*i.e.*, "sufficient physical security" as described in ¶ 16). While this does not mandate a universal, absolute level of security, one skilled in the art could, in any given instance, determine what was a sufficient level of security for some nodes and an insufficient level of security for others.

Although the claim terms considered in a vacuum might be considered relative, this relative nature does not preclude one of ordinary skill in the art from understanding the claim taken as a whole. MPEP 2173.02 ("[T]he examiner must consider the claim as a whole to determine whether the claim apprises one of ordinary skill in the art of its scope....") When looking at claim 1 as a whole, one skilled in the art would clearly understand that the method includes, among other things: (1) locating one or more nodes in a location deemed sufficiently secure, (2) locating one or more nodes in a location less secure than the sufficiently secure location, and (3) preventing management access to the secure network from nodes in the less secure location.

Reversal of the rejection of claim 1 and all claims depending therefrom (including claim 13) is therefore requested.

Claims 1, 18–19, 35, 72, and 76 were rejected for use of the term "substantive." The text of the exact rejection is:

> The term "substantive" in claims 1, 18, 19, 35, 72, and 76 is a relative term which renders the claim indefinite. The term "substantive" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. In this particular instance, one of ordinary skill in the art would be unable to determine what is considered substantive communication. As such, one of ordinary skill in the art would not be able to determine the scope of the claim. Therefore, claims 1, 18, 19, 35, 72, and 76 are rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

As noted in a prior response, the specification does provide sufficient guidance for one skilled in the art to determine the meaning of "substantive." The specification is replete with examples that explain what is meant by "substantive."

For example, ¶¶ 21 and 68 refer to "techniques for enhancing security and ***substantive*** operations." One of ordinary skill in the art would clearly understand this to distinguish between system overhead, such as security, and substantive operations, which would include the exchange of the underlying data. (Paragraph 149 clarifies that security is an overhead item.) Paragraph 169 teaches: "In the area of critical security, in order to be most secure, authentication must be completed prior to the exchange of ***substantive*** data or the granting of access to downstream data and services." One of ordinary skill in the art would clearly understand that authentication, a security communication, necessarily requires an exchange of data, but this must occur before the exchange of non-overhead data. Additionally, ¶ 82 explains that in the event of an NCE failure, ***substantive*** communication should be stopped until an NCE comes on line. One skilled in the art would understand that bringing an NCE on line would require the exchange of authentication and other security and configuration data before substantive communication, *i.e.*, non-overhead data, could resume.

Therefore, Applicant submits that one of ordinary skill in the art would understand the use of the term "substantive communication" as it appears in claims 1, 18–19, 35, 72, and 76. Reversal of the rejection of these claims is therefore requested.

B. Section 102(b) Novelty Rejection

Claims 1–13, 17–19, 35–47, 51–53, and 72–73 were rejected under § 102(b) as anticipated by Sudama. Applicants respectfully traverse all of these rejections.

Independent claim 1 was rejected as follows:

> Regarding claim 1, Sudama disclosed a method of operating a secure network having plurality of network nodes, each node comprising one or more ports (See Sudama Abstract), the method comprising the steps of: locating one or more nodes in a secure location (See Sudama Fig. 2); locating one or more nodes in a less secure location (See Sudama Col. 8 Paragraph 4); communicating selected management information from a primary configuration node to all other nodes in the secure network (See Sudama Col. 5 Paragraph 3), said communicating having the sub-steps of, a first port on a first node sending said management information to a second port on a second node via an communication media exclusively shared by said first port and said second port (See Sudama Col. 8 Paragraph 4 and Fig. 2); allowing no management access to said secure network from nodes located in said less secure locations (See Sudama Col. 8 Paragraph 4 and Fig. 2); determining a first list of nodes that may send or receive substantive communication in the secure network (See Sudama Col. 5 Paragraph 3); and prior to substantive communication between any two directly-connected ports, authenticating a link between said directly connected ports (See Sudama Col. 5 Paragraph 3).

Independent claim 1 recites numerous limitations not found in Sudama. Therefore, the rejection of this claim in view of Sudama is inappropriate. For example, Sudama contains no teaching or suggestion of "locating one or more nodes in a secure location." Examiner contends that this limitation can be found in Fig. 2. However, neither Fig. 2, nor the portions of the written description of Sudama that address Fig. 2 contain any teaching or suggestion relating to

the location of any of the components, much less any teaching or suggestion that any such locations are secure locations. In response, Examiner has stated that:

> Regarding applicants' argument that Sudama does not teach "locating one or more nodes in a secure location", or "locating one or more nodes in a less secure location" the examiner does not find the arguments persuasive. Sudama disclosed that "management operations can follow a trusted path downstream…however, no trusted path exists for routing management operations upstream." [Sudama Col. 8 Paragraph 4] As such, the upstream nodes are in a more secure location than the downstream locations. Therefore, the examiner does not find the arguments persuasive.

However, Sudama col. 8, ¶ 4 also does not teach anything about the location of any network nodes or the level of security of this location. The mere fact that a trusted communication path exists does not require or imply that one of the nodes be located in a secure location. Moreover, nothing else in Sudama appears to teach or suggest locating one or more nodes in a secure location. Therefore, rejection of claim 1 as anticipated by Sudama is improper.

Sudama also contains no teaching or suggestion of locating one or more nodes in a less secure location. The rejection reproduced above suggests that this limitation can be found in Sudama at col. 8, ¶ 4. However, this passage contains no teaching or suggestion relating to any sort of location, much less any teaching or suggestion of a less secure location. Examiner's rebuttal that the less secure location necessarily flows from the "trusted path downstream" has no basis in the reference. This passage teaches nothing about location, whether secure, less secure, or otherwise. Therefore, rejection of claim 1 as anticipated by Sudama is improper.

Obviously, because Sudama contains no teaching or suggestion of secure and less secure locations, it can contain no teaching or suggestion of "allowing no management access to said secure network from nodes located in said less secure locations." The rejection reproduced above again refers to Fig. 2 and col. 8, ¶ 4 as teaching this limitation of claim 1. However, in light Sudama's failure to teach or suggest anything relating to locations or security thereof, it is illogical to suggest that Sudama teaches management access restriction based on these locations. Rejection of claim 1 as anticipated by Sudama is therefore improper.

Sudama also fails to teach or suggest "determining a first list of nodes that may send or receive substantive communication in the secure network." Examiner points to col. 5, ¶ 3 of Sudama for this limitation. However, col. 5, ¶ 3 contains no teaching or suggestion of determining this type of list. Sudama does teach a global database that "provides a list of hosts for performing specified functions, the hosts' designated management servers and trusted routing paths between the management servers." However, this is not a list of nodes that may send or receive substantive communications. Sudama's list does not foreclose the possibility of other hosts engaging in substantive communication on the network.

In response, Examiner states that:

> Regarding applicants' argument that Sudama did not disclose "determining a first list of nodes that may send or receive substantive communication in the secure network", the examiner does not find the argument persuasive. The trusted routing paths of Sudama meet the limitation of the claim language as they determine which nodes may receive management operations. Therefore, the examiner does not find the argument persuasive.

However, this does not address the issue. Trusted routing paths have nothing to do with a list of all devices allowed to send or receive substantive communication in a secure network. Therefore, rejection of claim 1 as anticipated by Sudama is improper.

In view of the foregoing, reversal of the rejection of claim 1 is requested.

Independent claim 35 was rejected as follows:

> Regarding claim 35, Sudama disclosed a specific networking node operating in a secure network, said secure network having a plurality of network nodes, each node comprising one or more ports (See Sudama Fig. 2 and Abstract), said specific networking node comprising: a first port on said specific networking node for receiving selected management information from a primary configuration node (See Sudama Col. 5 Paragraph 3 and Fig. 2), said first port directly communicating with a second port on a second node via an communication media exclusively shared by said first port and said second port (See Sudama Fig. 2 and Col. 8 Paragraph 4); a memory for storing (i) management access information (See Sudama Col. 8 Paragraph 1), and

(ii) device connection information specifying nodes or ports that may send or receive substantive communication in the secure network (See Sudama Col. 8 Paragraph 1); and a processor for causing the authentication of the link between said first port and said second port prior to substantive communication between said first and second ports (See Sudama Col. 5 Paragraph 3).

Claim 35 requires, among other things, a primary configuration node "configured or adapted to exclusively control a defined set of management functions throughout said secure network." Examiner points to col. 5, ¶ 3 of Sudama as teaching exclusive control of a defined set of management functions throughout the network. However, neither this passage nor anything else in Sudama teaches that a primary configuration node exclusively controls a defined set of management functions throughout the network. In fact, the very passage cited by Examiner teaches that "[a]fter a management operation is received by a management server coupled to the point of access, … the originating management server transfers the management operation to the designated management server…." Thus, each of the various management servers has shared control, and thus no one server can have exclusive control of the functions being described in col. 5, ¶ 3. Moreover, Sudama clearly teaches multiple management servers M1, M2, M3, and M4 that each control management functions in particular parts of the network 2, S2, S3, and S4 (Fig. 2 and col. 8, ll. 48–67). The presence of multiple management servers with individual areas of responsibility throughout the network is clearly inconsistent with exclusive control of specified functions throughout the network. The rejection of claim 35 as anticipated by Sudama is therefore improper.

Claim 35 also requires "a memory for storing … device connection information specifying nodes or ports that may send or receive substantive communication in the secure network." Examiner points to col. 8, ¶ 1 as teaching this limitation. The list described in Sudama at col. 8, ¶ 1 is a list of trusted relations between the management servers. This list relates only to processing of management requests. There is no teaching or suggestion of the list "specifying nodes or ports that may send or receive substantive communication in the secure network." Many nodes or ports could send non-management substantive information while implementing the teaching of Sudama.

In response to this argument, Examiner states:

> Regarding applicants' argument that Sudama did not disclose "all of said devices carrying a list of all devices allowed on the network", the examiner does not find the argument persuasive. Sudama disclosed that each management server stored a list of trusted relations between the management servers. These lists include the devices of the network and therefore meet the limitations of the claim. As such, the examiner does not find the argument persuasive.

However, this misses the point. The plain language of the reference makes clear that the list only contains information about links between management servers. Even a casual reading of Sudama will show that the network is made up of nodes other than management servers that are allowed on the network, and yet these other nodes do not appear in the "list" cited by Examiner. Therefore, Sudama does not teach "a memory for storing … device connection information specifying nodes or ports that may send or receive substantive communication in the secure network," and the rejection of claim 35 as anticipated by Sudama is improper.

Reversal of the rejection of claim 35 is therefore requested.

Independent claim 73 was rejected as follows:

> Regarding claim 73, Sudama disclosed a network comprising: a plurality of devices including one or more switching and routing devices (See Sudama Col. 5 Paragraph 3), any two of said devices able to inter-communicate only by direct links between each other (See Sudama Fig. 2), all devices able to inter-communicate by forwarding communications through each other (See Sudama Col. 5 Paragraph 3); all of said devices capable of mutually authenticating directly connected links (See Sudama Col. 5 Paragraph 3); one or more pre-designated devices for facilitating management-level control of the network (See Sudama Col. 5 Paragraph 3); and all of said devices carrying a list of all devices allowed on the network (See Sudama Col. 8 Paragraph 1), wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network (See Sudama Col. 5 Paragraph 3).

Independent claim 73 requires, among other things, "a plurality of devices including one or more switching and routing devices, … all devices able to inter-communicate by forwarding communications through each other." Examiner contends that this limitation is taught by Sudama at col. 5, ¶ 3 and in Fig. 2. However, neither of these portions of Sudama teach or suggest that all devices inter-communicate by forwarding communications through each other. In fact, Sudama teaches exactly the opposite noting in col. 8, ll. 51–58 that:

> [M]anagement servers M1 through M4 [are] arranged in a hierarchical topology. Management operations can follow a trusted path downstream from M1 to M4, however, no trusted path exists for routing management operations upstream. For instance, M2–M4 cannot transmit a management operation to M1. Also, in this hierarchical topology, M4 cannot forward a request to any other management server M.

Because Sudama fails to teach or suggest "a plurality of switching and routing devices, … all devices able to inter-communicate by forwarding communications through each other" rejection of claim 73 as anticipated by Sudama is improper.

Claim 73 further requires that "all of said devices carry[] a list of all devices allowed on the network." Similar limitations were discussed above with respect to claims 1 and 35. Examiner contends that this limitation is taught by Sudama at col. 8, ¶ 1. However, this paragraph only discloses that a list of trusted relations between management servers is maintained in a database that may preferably be kept on each management server. The plain language of the reference makes clear that the list only contains information about links between management servers. However, the network clearly contains nodes other than management servers that are allowed to communicate. Yet, these other nodes do not appear in the "list." Thus, Sudama contains no teaching or suggestion of maintaining a list of all devices allowed on the network, and the anticipation rejection of claim 73 is improper.

In view of the foregoing, reversal of the rejection of claim 73 as anticipated by Sudama is requested.

Dependent claims 2–12 depending from claim 1 and dependent claims 36–46 depending from claim 35 were rejected as follows:

> Regarding claims 2-12, and 36-46, Sudama disclosed that said set of management functions comprising the recognition, operation and succession of primary configuration node (See Sudama Col. 5 Lines 20-21); node connection controls for designating nodes to participate in the secure network (See Sudama Col. 4 Lines 28-31), device connection controls that indicate port relationships in said secure network (See Sudama Col. 5 Lines 22-23), and management access controls that restrict management services to a defined set of endpoints (See Sudama Col. 5 Lines 20-23).

However, this rejection is inappropriate because Sudama does not teach "node connection controls for designating nodes to participate in the secure network." Moreover, Sudama does not teach "recognition, operation and succession of primary configuration node." The passage referred to by the Examiner relates to the distribution of management operations, not the succession of the management entity. Moreover, these dependent claims are also allowable for at least the reasons cited above with respect to their corresponding independent claims. Therefore, rejection of claims 2–12 and 36–46 is improper and reversal of this rejection is requested.

Dependent claim 13, depending from claim 1, and dependent claim 47, depending from claim 35 were rejected as follows:

> Regarding claims 13, and 47, Sudama disclosed that the step of allowing no management access to said secure network from nodes located in said less secure locations comprises the sub-step of distributing a MAC list to every node in said secure network, said MAC list comprising an indication of network endpoints from which management access is acceptable (See Sudama Col. 5 Paragraph 3 and Fig. 2).

Sudama teaches nothing about security of a location of any of the network components. Because Sudama contains no such teaching, it necessarily cannot teach the more precise step of distributing a list of network endpoints from which management access is acceptable based on the locations. Additionally, the passage cited relates to how a management request is handled by the distributed management servers. Nothing in the passage relates to whether or not a given

device is allowed to access the management servers. In fact, the cited passage seems to suggest that all devices on the network are allowed some access to at least one management server and that the management servers will sort out authorization to perform the specific task among themselves. In contrast, the language of claims 13 and 47 requires that management access be allowed only from designated nodes and, conversely, that management access be denied from nodes that are not so designated.

Dependent claims 18–19 and 52–53, depending from claims 1 and 35, respectively, were rejected as follows:

> Regarding claims 18 and 52, Sudama disclosed that the step of determining a first list of nodes that may send or receive substantive communication in the secure network comprises the sub-step of distributing a DCC list to every node in said secure network, said DCC list comprising definitions that logically bind a port on said primary configuration node to one or more other ports resident in the secure network (See Sudama Col. 5 Paragraph 3 and Col. 8 Paragraph 1 and Fig. 2).
>
> Regarding claims 19 and 53, Sudama disclosed that the step of determining a first list of nodes that may send or receive substantive communication in the secure network comprises the sub-step of distributing a DCC list to every node in said secure network, said DCC list comprising definitions that logically bind each port in said secure network to one or more other ports resident in said network (See Sudama Col. 5 Paragraph 3 and Col. 8 Paragraph 1 and Fig. 2).

At issue in both rejections is the claim limitation relating to a DCC list. Each of the referenced claims requires that the DCC list be distributed to every node in the secure network. Sudama does not disclose such a list. Column 8, ¶ 1 clearly states that "[t]hese lists, though maintained by a global procedure, would preferably be stored and accessible locally by each management server...." Sudama's lists are at most stored only by the management servers, and not by other network nodes. Rejection of claims 18–19 and 52–53 as anticipated by Sudama is therefore improper, and reversal of these rejections is therefore requested.

B. Section 103(a) Obviousness Rejections

The Office Action rejected various claims under various § 103(a) obviousness grounds. Applicants respectfully traverse all of them.

Independent claim 76 was rejected as follows:

> Regarding claim 76, the combination of Sudama and FIPS disclosed a routing device for receiving and directing information in a network (See Sudama Fig. 2), comprising: a public and private key pair (See FIPS Section 3.1.4); one or more ports for coupling to other routing devices and for authenticating said other routing devices and for communicating using said public and private key pair (See Sudama Fig. 2 and Col. 5 Paragraph 3 and the rejection of claim 22 above); a memory for storing a list of all said other routing devices that are allowed to substantively communicate on the network (See Sudama Col. 8 Paragraph 1); and a least one logical management access channel that may be disabled through network management control (See Sudama Col. 8 Paragraph 4).

Examiner again relies on Sudama at col. 8, ¶ 1 for teaching of "a memory for storing a list of all said other routing devices that are allowed to substantively communicate on the network." However, the "list" referred to by Examiner is not a list of routing devices allowed on the network, but rather a list of certain functions that are performed by certain hosts on the network. Sudama contains no teaching or suggestion that this list contains routing devices allowed on the network or, by extension, that routing devices not on the list are not allowed on the network. This missing limitation is not supplied by FIPS. Because the combination proposed fails to teach each element of the claim, the rejection under § 103 is improper.

Claim 76 further requires "at least one logical management access channel that may be disabled through network management control." Examiner contends that this limitation is taught by Sudama at col. 8, ¶ 4. However, neither this passage nor any other portion of Sudama teaches or suggests a logical management access channel that may be disabled through network management control. In his rebuttal, Examiner further explains:

> Regarding applicants' argument that Sudama did not disclose a "logical management channel" which may be disabled through network management control, the examiner does not find the argument persuasive. The fact that the management control of Sudama prevents upstream management communication, shows that the management communications are separate from non management communications and therefore in a "logical channel" and the upstream "channel" is disabled through the list of trusted paths. As such the examiner does not find the argument persuasive.

Examiner's rebuttal only bolsters the position that there is no management access channel that can be disabled through network management control. The "channel" to which Examiner refers is the upstream flow of management information. However, this is not a channel that can be enabled or disabled, but rather it is a channel that does not exist. Sudama provides no mechanism for an upstream channel in the first place. This is not a channel that can be disabled; it is the absence of a channel. Furthermore, FIPS fails to teach or suggest such a logical management access channel. Therefore, the proposed combination further fails to teach or suggest each limitation of claim 76, and the rejection of claim 76 is improper.

Reversal of the rejection of claim 76 as obvious over Sudama and FIPS is therefore requested.

Independent claim 79 was rejected as follows:

> Regarding claim 79, the combination of Sudama and FIPS disclosed a network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and

succession of the network configuration entity and (ii) switch connection controls for designating devices to participate in the secure network (See Sudama Col. 5 Paragraph 3), said network configuration entity comprising; a memory for storing an NCE list, said NCE list comprising an indication of each device in the network that may operate as said network configuration entity (See Sudama Col. 5 Paragraph 3); an SCC list, said SCC list comprising an indication of each device allowed to participate in said secure network (See Sudama Col. 5 Paragraph 3); a first secret fact; a first port for sending said secret fact to a second switch; a second port for receiving, a second-type derivative of said first secret fact from said second switch, pre-defined information about said second switch, and a third-type derivative of said pre-defined information about said second switch; and a processor for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said second switch and said third-type derivative of said pre-defined information about said second switch (See the rejection of claim 22 above).

However, there are at least two limitations of claim 79 that are not met by the combination of Sudama and FIPS. One such limitation is a memory storing "an NCE list … comprising an indication of each device in the network that may operate as said network configuration entity." Examiner points to Sudama at col. 5, ¶ 3. As discussed above, this list in Sudama is a "list of hosts for performing specified functions, the hosts' designated management servers and trusted routing paths between the management servers." Nowhere does Sudama teach that the list indicates which device or devices can serve as a network configuration entity. Even if this is implicit in "a list of hosts for performing specified functions," which is not conceded, the list clearly does not meet the requirements of the SCC list. The SCC list must indicate each device allowed on the secure network. The list of Sudama does not specify each device that may communicate in the network, it only lists certain devices that perform certain functions. Nowhere does Sudama teach or suggest only devices in this list are allowed on the network.

Furthermore, FIPS fails to disclose either such list. Thus, the combination of Sudama and FIPS fails to teach the NCE and SCC list limitations of claim 79, and the rejection of claim 79 is improper.

Reversal of the rejection of claim 79 is therefore requested.

Claim 72 was rejected under § 103 as obvious over Sudama in view of U.S. Patent 5,694,615 to Thapar ("Thapar") as follows:

> Claims 72 and 74 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama as applied to claim 73 above, and further in view of Thapar et al. (US Patent Number 5,694,615) hereinafter referred to as Thapar.
>
> Sudama disclosed a method of securing a fabric, said fabric having a plurality of switches all communicatively coupled together, said method comprising the steps of: only allowing communication between pre-defined pairs of said devices as specified by a network operator (See Sudama Col. 5 Paragraph 3); and only allowing substantive communication between devices that are on a pre-defined list of allowed devices (See Sudama Col. 5 Paragraph 3), said pre-defined list stored on a memory in each of said plurality of devices (See Sudama Col. 8 Paragraph 1); and only allowing substantive communication between directly connected ports that have been mutually authenticated (See Sudama Col. 5 Paragraph 3), but failed to disclose the system being used in a fibre channel.
>
> Thapar teaches that the fibre channel addresses the need for very fast data transfers (See Thapar Col. 1 Lines 18-26).
>
> It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Thapar in the communication network of Sudama by replacing the routers of Thapar with Fibre Channel routers. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow for very fast transfers of large volumes of data.

As discussed above, this rejection relies on Sudama at col. 5, ¶ 3 for "only allowing substantive communication between devices that are on a pre-defined list of allowed devices." However, the list of Sudama only specifies that certain hosts perform certain functions. The list does not specify the universe of devices that may communicate on the network. Thus, Sudama's list does not meet this limitation of claim 72. Thapar also fails to teach or suggest this limitation. Therefore, the rejection of claim 72 as obvious over Sudama and Thapar is inappropriate.

An additional limitation of claim 72 requires "only allowing substantive communication between directly connected ports that have been mutually authenticated." Sudama and Thapar, whether separately or in combination, fail to meet this limitation. Examiner cites Sudama at col. 5, ¶ 3, which does state that management operations are only permitted between management servers that have been mutually authenticated. However, Sudama does not require that any substantive communications other than management communications take place only over mutually authenticated links. Thapar does not supply this missing limitation. Therefore, the rejection of claim 72 as obvious over Sudama and Thapar is inappropriate.

Reversal of the rejection of claim 72 is therefore requested.

F. CONCLUSION

For the reasons stated above, Applicants respectfully submit that the rejections should be reversed. Additionally, to the extent specific claims have not been addressed, these claims depend from one or more claims that are specifically addressed, and are therefore patentable for at least the same reasons as the claims specifically addressed. Applicants further believe that they have complied with each requirement for an appeal brief.

In the course of the foregoing discussions, Applicants may have at times referred to claim limitations in shorthand fashion, or may have focused on a particular claim element. This discussion should not be interpreted to mean that the other limitations can be ignored or dismissed. The claims must be viewed as a whole, and each limitation of the claims must be considered when determining the patentability of the claims. Moreover, it should be understood that there may be other distinctions between the claims and the prior art which have yet to be raised, but which may be raised in the future.

If any fees are required or have been overpaid, please appropriately charge or credit those fees to Deposit Account Number 501922, referencing docket number 112-0039US.

Respectfully submitted,

/Billy C. Allen III/

March 26, 2007

Filed Electronically

Billy C. Allen III, Reg. No. 46,147
Wong, Cabello, Lutsch,
Rutherford & Brucculeri, L.L.P.
20333 State Hwy 249, Suite 600
Houston, TX 77070
832-446-2409

VIII. CLAIMS APPENDIX

1. (Previously Presented) A method of operating a secure network having plurality of network nodes, each node comprising one or more ports, the method comprising the steps of:

locating one or more nodes in a secure location;

locating one or more nodes in a less secure location;

communicating selected management information from a primary configuration node to all other nodes in the secure network, said communicating having the sub-steps of,

a first port on a first node sending said management information to a second port on a second node via a communication media exclusively shared by said first port and said second port;

allowing no management access to said secure network from nodes located in said less secure locations;

determining a first list of nodes that may send or receive substantive communication in the secure network; and

prior to substantive communication between any two directly-connected ports, authenticating a link between said directly connected ports.

2. (Original) The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising the recognition, operation and succession of primary configuration node.

3. (Original) The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, (ii) node connection controls for designating nodes to participate in the secure network, (iii) device connection controls that indicate port relationships in said secure network, and (iv)

management access controls that restrict management services to a defined set of endpoints.

4. (Original) The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of the primary configuration node, and (ii) node connection controls for designating nodes to participate in the secure network,.

5. (Original) The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, and (ii) device connection controls that indicate port relationships in said secure network.

6. (Original) The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, and (ii) management access controls that restrict management services to a defined set of endpoints.

7. (Original) The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) node connection controls for designating nodes to participate in the secure network, and (ii) device connection controls that indicate port relationships in said secure network.

8. (Original) The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising, (i) node connection controls for designating nodes to participate in the secure network and (ii)

management access controls that restrict management services to a defined set of endpoints.

9. (Original) The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) device connection controls that indicate port relationships in said secure network, and (ii) management access controls that restrict management services to a defined set of endpoints.

10. (Original) The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, (ii) node connection controls for designating nodes to participate in the secure network, and (iii) device connection controls that indicate port relationships in said secure network.

11. (Original) The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node, (ii) node connection controls for designating nodes to participate in the secure network, and (iii) management access controls that restrict management services to a defined set of endpoints.

12. (Original) The invention of claim 1 wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network, said set of management functions comprising (i) the recognition, operation and succession of said primary configuration node (ii) device connection controls that indicate port relationships in said secure network, and (iii) management access controls that restrict management services to a defined set of endpoints.

13. (Original) The invention of claim 1 wherein the step of allowing no management access to said secure network from nodes located in said less secure locations comprises the sub-step of distributing a MAC list to every node in said secure network, said MAC list comprising an indication of network endpoints from which management access is acceptable.

14. (Original) The invention of claim 13 wherein said network endpoints comprise IP addresses.

15. (Original) The invention of claim 14 wherein said IP addresses are associated with access from SNMP or Telnet or HTTP or API.

16. (Original) The invention of claim 13 wherein said network endpoints comprise uniquely identified ports.

17. (Original) The invention of claim 13 wherein said network endpoints comprise uniquely identified nodes resident in said secure network.

18. (Original) The invention of claim 1 wherein the step of determining a first list of nodes that may send or receive substantive communication in the secure network comprises the sub-step of distributing a DCC list to every node in said secure network, said DCC list comprising definitions that logically bind a port on said primary configuration node to one or more other ports resident in the secure network.

19. (Original) The invention of claim 1 wherein the step of determining a first list of nodes that may send or receive substantive communication in the secure network comprises the sub-step of distributing a DCC list to every node in said secure network, said DCC list comprising definitions that logically bind each port in said secure network to one or more other ports resident in said network.

20. (Original) The invention of claim 19 wherein said ports are identified by a unique number.

21. (Original) The invention of claim 20 wherein said unique number is a world-wide-name.

22. (Original) The invention of claim 1 wherein said directly connected ports are said first port and said second port and wherein the step of authenticating a link between said directly connected ports comprises the sub-steps of:

sending a first fact from said first port to said second port;

at said second node, creating a second-type derivative of said first fact,

sending said second-type derivative of said first fact from said second port to said first port;

at said first node, storing said second-type derivative of said first fact in a first memory;

sending a second fact from said second port to said first port;

at said first node, creating a first-type derivative of said second fact;

sending said first-type derivative of said second fact from said first port to said second port;

at said second node, storing said first-type derivative of said second fact in a second memory;

sending defined information concerning said first node from said first port to said second port;

sending a third-type derivative of said defined information concerning said first node from said first port to said second port;

at said second node, comparing said defined information concerning said first node with said third-type derivative of said defined information concerning said first node;

at said second node, comparing said first type derivative of said second fact with said second fact;

sending defined information concerning said second node from said second port to said first port;

sending a third-type derivative of said defined information concerning said second node from said second port to said first port;

at said first node, comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node; and

at said first node, comparing said second type derivative of said first fact with said first fact.

23. (Original) The method of claim 22 wherein the step of comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node, comprises the sub-steps of:

reversing the derivation of the third-type derivative of said defined information concerning said second node; and

comparing the result of said reversal with said defined information concerning said second node.

24. (Original) The method of claim 22 wherein the step of comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node, comprises the sub-steps of:

making a third-type derivative of said defined information concerning said second node; and

comparing the made third-type derivative with the received third-type derivative.

25. (Original) The method of claim 22 wherein the step, at said second node, of creating a second-type derivative of said first fact comprises the sub-steps of:

encoding said first fact to yield an encoded first fact; and

encrypting said encoded first fact.

26. (Original) The method of claim 25 wherein said encoding is performed by applying a hash function.

27. (Original) The method of claim 25 wherein said encrypting is performed using a private key unique to said second node.

28. (Original) The method of claim 22 wherein said defined information concerning said first node comprises encryption key information.

29. (Original) The method of claim 28 wherein said encryption key information comprises a public key uniquely associated with said first node.

30. (Original) The method of claim 22 wherein said third-type derivative is associated with both said second node and said first node.

31. (Original) The method of claim 30 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority associated with said first node and said second node.

32. (Original) The method of claim 30 wherein said third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority being the manufacturer of either said first node or said second node.

33. (Original) The method of claim 22 wherein the step, at said second node, of comparing said defined information concerning said first node with said third-type derivative of said defined information concerning said first node, comprises the sub-steps of:

reversing said third-type derivative of said defined information concerning said first node yielding a reversed third-type derivative; and

comparing said reversed third-type derivative with said defined information concerning said first node.

34. (Original) The method of claim 33 wherein said step of reversing said third-type derivative is performed using a public key uniquely associated with an encryption key authority, said encryption key authority associated with said first node and said second node.

35. (Previously Presented) A specific networking node operating in a secure network, said secure network having a plurality of network nodes, each node comprising one or more ports, said specific networking node comprising:

a first port on said specific networking node for receiving selected management information from a primary configuration node, said first port directly communicating with a second port on a second node via a communication media exclusively shared by said first port and said second port;

a memory for storing (i) management access information, and (ii) device connection information specifying nodes or ports that may send or receive substantive communication in the secure network; and

a processor for causing the authentication of the link between said first port and said second port prior to substantive communication between said first and second ports;

wherein said primary configuration node is configured or adapted to exclusively control a defined set of management functions throughout said secure network.

36. (Previously Presented) The invention of claim 35 wherein said set of management functions comprises the recognition, operation and succession of primary configuration node.

37. (Previously Presented) The invention of claim 35 wherein said set of management functions comprises (i) the recognition, operation and succession of said primary configuration node, (ii) node connection controls for designating nodes to participate in the secure network, (iii) device connection controls that indicate port relationships in said secure network, and (iv) management access controls that restrict management services to a defined set of endpoints.

38. (Previously Presented) The invention of claim 35 wherein said set of management functions comprises (i) the recognition, operation and succession of the primary configuration node, and (ii) node connection controls for designating nodes to participate in the secure network,.

39. (Previously Presented) The invention of claim 35 wherein said set of management functions comprises (i) the recognition, operation and succession of said primary configuration node, and (ii) device connection controls that indicate port relationships in said secure network.

40. (Previously Presented) The invention of claim 35 wherein said set of management functions comprises (i) the recognition, operation and succession of said primary configuration node, and (ii) management access controls that restrict management services to a defined set of endpoints.

41. (Previously Presented) The invention of claim 35 wherein said set of management functions comprises (i) node connection controls for designating nodes to participate in the secure network, and (ii) device connection controls that indicate port relationships in said secure network.

42. (Previously Presented) The invention of claim 35 wherein said set of management functions comprises, (i) node connection controls for designating nodes to participate in the secure network and (ii) management access controls that restrict management services to a defined set of endpoints.

43. (Previously Presented) The invention of claim 35 wherein said set of management functions comprises (i) device connection controls that indicate port relationships in said secure network, and (ii) management access controls that restrict management services to a defined set of endpoints.

44. (Previously Presented) The invention of claim 35 said set of management functions comprises (i) the recognition, operation and succession of said primary configuration node, (ii) node connection controls for designating nodes to participate in the secure network, and (iii) device connection controls that indicate port relationships in said secure network.

45. (Previously Presented) The invention of claim 35 wherein said set of management functions comprises (i) the recognition, operation and succession of said primary

configuration node, (ii) node connection controls for designating nodes to participate in the secure network, and (iii) management access controls that restrict management services to a defined set of endpoints.

46. (Previously Presented) The invention of claim 35 wherein said set of management functions comprises (i) the recognition, operation and succession of said primary configuration node (ii) device connection controls that indicate port relationships in said secure network, and (iii) management access controls that restrict management services to a defined set of endpoints.

47. (Previously Presented) The invention of claim 35 wherein said management access information comprises a MAC list, said MAC list comprising an indication of network endpoints from which management access is acceptable.

48. (Original) The invention of claim 47 wherein said network endpoints comprise IP addresses.

49. (Original) The invention of claim 48 wherein said IP addresses are associated with access from SNMP or Telnet or HTTP or API.

50. (Original) The invention of claim 47 wherein said network endpoints comprise uniquely identified ports.

51. (Original) The invention of claim 47 wherein said network endpoints comprise uniquely identified nodes resident in said secure network.

52. (Original) The invention of claim 35 wherein said device connection information comprises a DCC list, said DCC list comprising definitions that logically bind a port on said primary configuration node to one or more other ports resident in the secure network.

53. (Original) The invention of claim 35 wherein said device connection information comprises a DCC list, said DCC list comprising definitions that logically bind each port in said secure network to one or more other ports resident in said network.

54. (Original) The invention of claim 53 wherein said one or more other ports are identified by a unique number.

55. (Original) The invention of claim 54 wherein said unique number is a world-wide-name.

56. (Original) The invention of claim 35 wherein said specific networking node further comprises:

a second memory for storing a first secret fact;

a third port for sending said secret fact to a third node;

a fourth port for receiving,

a second-type derivative of said first secret fact from said third node,

pre-defined information about said third node, and

a third-type derivative of said pre-defined information about said third node; and

said processor also for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said third node and said third-type derivative of said pre-defined information about said third node.

57. (Original) The invention of claim 56 wherein said third port and said fourth port are the same port.

58. (Original) The invention of claim 56 wherein said comparison, between said first secret fact and said second-type derivative of said first secret fact, includes reversing the derivative nature of said second-type derivative of said first secret fact.

59. (Previously Presented) The invention of claim 56 wherein said comparison, between said first secret fact and said second-type derivative of said first secret fact, includes creating a second-type derivative of said first secret fact.

60. (Original) The invention of claim 56 wherein said second-type derivative is associated with said third node.

61. (Original) The invention of claim 56 wherein said third-type derivative is associated with said specific networking node and said third node.

62–71. (Cancelled)

72. (Previously Presented) A method of securing a fabric, said fabric having a plurality of switches all communicatively coupled together, said method comprising the steps of:

only allowing communication between pre-defined pairs of said switches as specified by a network operator; and

only allowing substantive communication between devices that are on a pre-defined list of allowed devices, said pre-defined list stored on a memory in each of said plurality of switches; and

only allowing substantive communication between directly connected ports that have been mutually authenticated.

73. (Original) A network comprising:

a plurality of devices including one or more switching and routing devices, any two of said devices able to inter-communicate only by direct links between each other, all devices able to inter-communicate by forwarding communications through each other;

all of said devices capable of mutually authenticating directly connected links;

one or more pre-designated devices for facilitating management-level control of the network; and

all of said devices carrying a list of all devices allowed on the network.

74. (Original) The invention of claim 73 where the network is a Fibre Channel fabric and all the devices are routing and switching devices.

75. (Original) The invention of claim 73 wherein said pre-designated devices are each in a room having a locking mechanism to control human ingress and egress.

76. (Previously Presented) A routing device for receiving and directing information in a network, comprising:

a public and private key pair;

one or more ports for coupling to other routing devices and for authenticating said other routing devices and for communicating using said public and private key pair;

a memory for storing a list of all said other routing devices that are allowed to substantively communicate on the network; and

at least one logical management access channel that may be disabled through network management control.

77. (Original) The invention of claim 76 where a certificate authority for the public and private key pair is not the entity controlling management access to said routing device

78. (Original) The invention of claim 76 further comprising a memory for storing distributed time service information.

79. (Previously Presented) A network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network, said secure network comprising a plurality of switching devices, said set of management functions comprising (i) the recognition, operation and succession of the network configuration entity and (ii) switch connection controls for designating devices to participate in the secure network, said network configuration entity comprising;

a memory for storing

an NCE list, said NCE list comprising an indication of each device in the network that may operate as said network configuration entity;

an SCC list, said SCC list comprising an indication of each device allowed to participate in said secure network; and

a first secret fact;

a first port for sending said secret fact to a second switch;

a second port for receiving,

a second-type derivative of said first secret fact from said second switch,

pre-defined information about said second switch, and

a third-type derivative of said pre-defined information about said second switch; and

a processor for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said second switch and said third-type derivative of said pre-defined information about said second switch.

80. (Original) The invention of claim 79 wherein said first port and said second port are the same port.

81. (Original) The invention of claim 79 wherein said comparison, between said first secret fact and said second-type derivative of said first secret fact, includes reversing the derivative nature of said second-type derivative of said first secret fact.

82. (Original) The invention of claim 79 wherein said comparison, between said first secret fact and said second-type derivative of said first secret fact, includes creating a second-type derivative of said first secret fact.

83. (Original) The invention of claim 79 wherein said second-type derivative is associated with said second switch.

84. (Original) The invention of claim 79 wherein said third-type derivative is associated with said network configuration entity and said second switch.

85. (Original) The invention of claim 79 wherein said pre-defined information about said second switch comprises encryption key information.

86. (Original) The invention of claim 79 wherein said first secret fact is a random number.

87. (Original) The invention of claim 79 wherein said first secret fact is a nonce.

88–89. (Cancelled)

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.